S. LANE TUCKER
United States Attorney

SETH M. BEAUSANG
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: seth.beausang@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. VIRTUAL CURRENCY ASSETS SEIZED FROM: BINANCE US ACCOUNTS WITH USER IDENTIFIERS ENDING IN 5099, 9181, & 2269; and FTX TRADING LTD. ACCOUNTS WITH USER IDENTIFIERS ENDING IN 9862 & 1919, Defendants.	)	No. 3:23-cv-00079-JMK

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

The United States of America, by its attorneys, alleges the following in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

Nature of the Action

1. This is a civil action *in rem* to forfeit property to the United States under the provisions of 18 U.S.C. §§ 981(a)(1)(A) & (C), for violations of 18 U.S.C. §§ 1343 & 1956.

The Defendant *In Rem*

2. The defendant property are virtual currency assets seized pursuant to seizure warrants served on October 6, 2022, (collectively, "Defendant *in rem*"), specifically assets seized from:

a. Binance US account with user identifier ending in 5099, namely, approximately 0.9998 BTC;

b. Binance US account with user identifier ending in 9181, namely, approximately 0.67783418 BNB, 13059998.65 SHIB, 215.9717936 DOT, 12478384.27 LUNC, 1.71984582 BTC, 1.00654101 ETH, 230.9966431 LTC, 349.231396 LINK, 18147.58806 ADA, 52.340356 LUNA, 11619.25919 XRP, and 4363.900482 TRX;

c. Binance US account with user identifier ending in 2269, namely, approximately 41.07621525 ETHW, 0.00931 BETH, 12081.94595 SGB, 451.546 XNO, 108187889.8, 586.32161808 DOT, 8453.486334 TRX, 387128.81937 ADA, 42173.1408 ZIL, 4.7387963 BTC, 14.08070163 BNB, 82.96118542 ETH, 99NEO, 2659.751 XLM, 2.99155673 XMR;

d. FTX Trading Ltd. account with user identifier ending in 9863, namely, approximately 6.97980254 ETH; and

e. FTX Trading Ltd. account with user identifier ending in 1919, namely approximately 1578.210263 USDC, 9.999 ETH, 0.16641477 BTC, and 51.385 FTT;

3. Defendant *in rem* is presently in the custody of the FBI in the District of Alaska.

Jurisdiction and Venue

4. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a).

5. Venue is proper in this Court under 28 U.S.C. § 1395 because the acts or omissions giving rise to the forfeiture occurred, at least in part in the District of Alaska.

Background

6. Under 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of [18 U.S.C. §§ 1956], or any property traceable to such property" is subject to civil forfeiture to the United States. In addition, under 18 U.S.C. § 981(a)(1)(C), with cross references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of" of a wire fraud offense or offenses committed in violation of 18 U.S.C. § 1343 is subject to civil forfeiture to the United States.

7. Defendant *in rem* is subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A) because it was involved in the commission of a money laundering offense or offenses committed in violation of 18 U.S.C. § 1956, and subject to forfeiture under 18

U.S.C. § 981(a)(1)(C) because it constitutes proceeds, or property traceable to proceeds, of a wire fraud offense or offenses committed in violation of 18 U.S.C. § 1343.

8. On October 6, 2022, an application was made by FBI Special Agent Frank D. Reid, Jr. to the U.S. District Court for the District of Alaska for combined criminal and civil forfeiture seizure warrants for the following assets:

a. Any and all assets contained within the Binance US[1] accounts associated with the following Binance User Identifiers ("UID"): 10282269 ("Target Property 1"), 120689181 ("Target Property 2"), and 11185099 ("Target Property 3").

b. Any and all assets within the FTX Trading Ltd.[2] ("FTX") accounts associated with FTX account numbers 45319863 ("Target Property 4") and 44601919 ("Target Property 5").[3]

9. On October 6, 2022, United States Magistrate Judge Matthew M. Scoble found probable cause that the TARGET PROPERTIES were subject to civil and criminal forfeiture to the United States and issued seizure warrants 1:22-mj-00081-MMS and 1:22-mj- 00082-MMS for the TARGET PROPERTIES.

[1] Binance is an online cryptocurrency exchange platform; URL www.binance.com. Binance was founded in 2017 and is registered in the Cayman Islands.
[2] FTX Trading Ltd is an online cryptocurrency exchange platform; URL www.ftx.com. FTX is a cryptocurrency exchange that was founded in 2019. FTX is incorporated in Antigua and Barbuda and headquartered in The Bahamas.
[3] The Binance and FTX accounts are collectively referred to as the "TARGET PROPERTIES."

Forfeiture Authority

10. Defendant *in rem* is subject to civil forfeiture if the United States shows probable cause to believe that underlying wire fraud or subsequent money laundering conduct occurred, and that the Defendant *in rem* has a nexus to that offense—namely, that the Defendant *in rem* contains assets that constitute wire fraud proceeds or property traceable to such proceeds, were involved in money laundering or are traceable to property involved in money laundering, or both. *See* 18 U.S.C. §§ 981(a)(1)(A) & (C). Probable cause means Probable cause is sufficient information to convince a "prudent person ... that there was a fair probability" that the res is subject to forfeiture. *United States v. Lopez*, 482 F.3d 1067, 1072 (9th Cir. 2007).

11. As set forth herein, there is a fair probability that the Defendant *in rem* includes assets that both (a) are traceable to proceeds of a wire fraud scheme involving financial fraud and (b) were commingled with assets from other victims of wire fraud in an attempt to conceal the source of the Defendant *in rem* and facilitate this scheme. Defendant *in rem* is therefore subject to forfeiture as proceeds of wire fraud and because it was involved in apparent concealment money laundering conduct. *See, e.g., United States v. Guerrero*, 2021 WL 2550154, *9 (N.D. Ill. June 22, 2021) (money from unknown source that was commingled with fraud proceeds facilitated the concealment laundering of the fraud proceeds and, accordingly, property acquired with the commingled funds was forfeitable as property traceable to property involved in a money laundering offense); *United States v. Lazarenko*, 564 F.3d 1026, 1035 (9th Cir. 2009)

("[I]n a money laundering charge, the commingling of tainted money with clean money taints the entire account.").

Background on Cryptocurrency

12. The following relevant terms and definitions are used herein:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrencies are Bitcoin (or "BTC"), Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies exist on a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[4] Cryptocurrency, itself, is not illegal in the United States.

[4] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

b. As previously stated, bitcoin[5] (or BTC) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded on the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (*i.e.*, online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people.

c. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, bitcoin allows

[5] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

d. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26 to 35 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address's private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

e. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes—for example, as payment for illegal goods and services and to commit money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases. The value of bitcoin is generally much more volatile than that of fiat currencies.

f. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of

forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[6] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase).

g. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to the United States Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and

[6] A QR code is a matrix barcode that is a machine-readable optical label.

exchangers, including an individual exchanger operating as a business, are considered money services businesses.[7] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat-currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

h. Some companies offer cryptocurrency wallet services, which allow users to download a digital wallet application onto their smart phone or other digital

[7] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the specific device on which the wallet application was installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

Background of Investigation

13. On June 21, 2022, the FBI met with a son and daughter of Victim A and Victim B, (hereinafter collectively referred to as the "Victims"), who fell victim to a financial fraud scheme wherein they wired a total of $1,195,000 to a California Bank under the false pretense that doing so would keep their money safe from hackers. Victim A and Victim B are currently 90 and 92 years of age, respectively.

14. According to interviews of the Victims' children, who were authorized to discuss the Victims' financial affairs, Victim A was working on a personal computer when a pop-up or dialogue box appeared on the screen purporting to be from Microsoft Corporation. The dialogue box stated that the Victims' computer had been compromised and included a telephone number for the Victims to call for assistance. The Victims called the number and spoke to what they believed were two different individuals: a person who claimed to be an employee of Microsoft, and later, a person who claimed to be an employee of Morgan Stanley where the Victims held an account. (These unidentified individuals are hereinafter collectively referred to as the "scammers"). The scammers informed the Victims that the Victims' computer, personal information, and financial accounts had been compromised and that they needed to move their money to keep it safe. The Victims allowed the scammers to have remote access to Victim A's computer and cellphone utilizing a screensharing software the Victims were instructed to download by the scammers. The scammers requested and were provided with a copy of Victim A's driver's license, as well as other sensitive personally identifying information, as well as two-factor authentication numbers related to their online banking accounts, which allowed the scammers to view all of the accounts belonging to the Victims.

15. According to the Victims, the scammers told the Victims that the Victims needed to move their money from the Victims' accounts to new accounts for a temporary period to protect their retirement savings. Specifically, the scammers told Victim A that the Victims' Morgan Stanley Retirement Accounts had been compromised, as well as their Social Security Numbers. In order to protect their investments, the Victims were

advised they needed to wire all of their money to a government account to keep it safe. Once the issue was resolved, the money would be returned in approximately 60 days.

16. The scammers instructed the Victims regarding the aforementioned plan to protect their investments during one of the many telephone conversations that took place. Specifically, the scammers provided bank account and reference numbers for each wire transfer and told the Victims to say, as well as what not to say, if questioned by their financial institutions. The scammers told the Victims that the use of cryptocurrency was part of the process to keep the Victims' money safe. The scammers, in conjunction with the Victims who acted at the direction of the scammers, converted the Victims' funds to cryptocurrency, then transferred the cryptocurrency to virtual wallets outside the Victims' control.

17. The scammers instructed and assisted Victim A with setting up an account at the virtual currency exchange Binance US for the purpose of converting Victims' money to cryptocurrency (the "Victims' Binance US Account"). According to publicly available information, Binance US, also known as BAM Trading Services (hereinafter "Binance US"), is a cryptocurrency service provider that provides "secure and reliable access to the world's most popular cryptocurrencies." Binance US is headquartered in Palo Alto, California.[8]

18. Binance US is an American subsidiary of Binance, the world's largest cryptocurrency exchange by trading volume. Binance stopped accepting U.S.

[8] From information on the Binance US website *www.binance.us*.

users in 2019 and announced it would instead partner with a U.S.-based version of its platform called Binance US. Binance US was started under a partnership with the FinCEN-registered BAM Trading Services as part of its move into the U.S. market.[9]

19. The scammers provided Victim A with an account number for a Silvergate Bank account that was linked to the Victims' Binance US Account. Per the Victims' children, the money was wired from one of the Victims' personal bank accounts on deposit with Wells Fargo.[10] Wells Fargo Bank was one of the banking institutions the Victims used for their personal banking. The funds from the Victims' Wells Fargo bank account were then wired into the Victims' Binance US Account pursuant to the instructions from the scammers. The scammers instructed Victim A to make the transfers and provide the scammers with the wire transfer reference code, which was required to complete the transaction in the Victims' Binance US Account. In total, $1,195,500 dollars were wired from the Victims' Wells Fargo account to the Victims' Binance US Account between approximately April 13, 2022 through May 20, 2022.

20. At the direction of the scammers, the Victims, while in the Districts of Arizona and Alaska, caused the following wire transfers to be sent from their Wells

[9] From information on the Time.com website *https://time.com/nextadvisor/investing/cryptocurrency/binance-us-review/*.

[10] Wells Fargo & Company is an American multinational financial services company with corporate headquarters in San Francisco, California; operational headquarters in Manhattan; and managerial offices throughout the United States and internationally.

Fargo account to the Binance US correspondent bank located in California, Silvergate Bank[11]:

Date[12]	Transfer Amount
4/13/2022	$500
4/14/2022	$300,000
4/21/2022	$400,000
4/29/2022	$100,000
5/06/2022	$90,000
5/13/2022	$230,000
5/20/2022	$75,000

21. The wire transfers that originated in the District of Alaska occurred on May 13, 2022 and May 20, 2022, in the total amount of $305,000.

22. After the funds were wired to the Silvergate Bank account, the scammers began purchasing bitcoin in $10,000 increments from the Victims' Binance US Account set up in Victim A's name. Each transaction incurred a $50 processing fee. The scammers explained to the Victims that they were required to convert the money this way and then again confirmed the money was going to a government account. When Victim A asked about all of the processing fees and potential tax consequences for withdrawing the funds,

[11] That the Victims initiated bank wire transfers from the District of Alaska to a bank in California establishes a fair probability that the wire transfers actually crossed a state line. *See, e.g.*, *United States v. Kieffer*, 681 F.3d 1143, 1154 (10th Cir. 2012) ("The presence of end users in different states, coupled with the very character of the internet, render this inference permissible even absent evidence that only one host server delivered web content in these two states."). In addition, bank wire transfers usually require the use of one or more interstate wire communications because the parties to the transaction, including the originator (in this case, the Victims), the originator's bank, the beneficiary bank, the beneficiary, and the processor—often the Federal Reserve Banks's Fedwire system—are typically geographically dispersed. In this case, the Victims were located in Arizona and Alaska. Fedwire data centers are located in New Jersey and Texas, and transfers are processed in a multiple steps. As such, it is reasonable to believe that some portion of the Victims' wire transfers were transmitted in interstate commerce.

[12] The dates included in this chart are based on the Victims' statements.

the scammers continued to reassure them that all of the funds would be returned to include any fees incurred.

23. The scammers were able to gain access to the Victims' Binance US Account by using two-factor authentication.[13] This included a code being sent to Victim A's personal cellular phone and the second code being sent to a Google Authenticator[14] controlled by the scammers. For every transaction that took place, the codes from the two-factor authentication had to be entered for the transaction to proceed. To get the code off Victim A's cellular phone, the scammers either viewed the text messages sent to Victim A's cellular telephone via the screensharing software previously installed at the scammers direction or Victim A would provide the code over the phone as they spoke. The second code was sent to the Google Authenticator controlled by the scammers.

24. The Victims' children provided the FBI with a summary of the financial transactions from the Victims' accounts, including the transfers into the accounts. In summary, the information provided contains US Dollar (USD) deposit confirmation information, cryptocurrency trade confirmation data, and account verification correspondence. Included in the summary report were three separate transactions where

[13] Two-factor authentication, sometimes referred to as *two-step verification* or *dual-factor authentication*, is a security process in which users provide two different authentication factors to verify themselves. (*https://www.techtarget.com/searchsecurity/definition/two-factor-authentication*)

[14] Google Authenticator is a mobile security application based on two-factor authentication that helps to verify user identities before granting them access to websites and services. (*https://www.techtarget.com/searchsecurity/definition/Google-Authenticator*)

the funds that were converted to bitcoin were sent to three separate addresses in the following transactions:

a. 4/22/2022 – Withdrawal 17.49835220 (bitcoin) to wallet "**bc1qf34**"

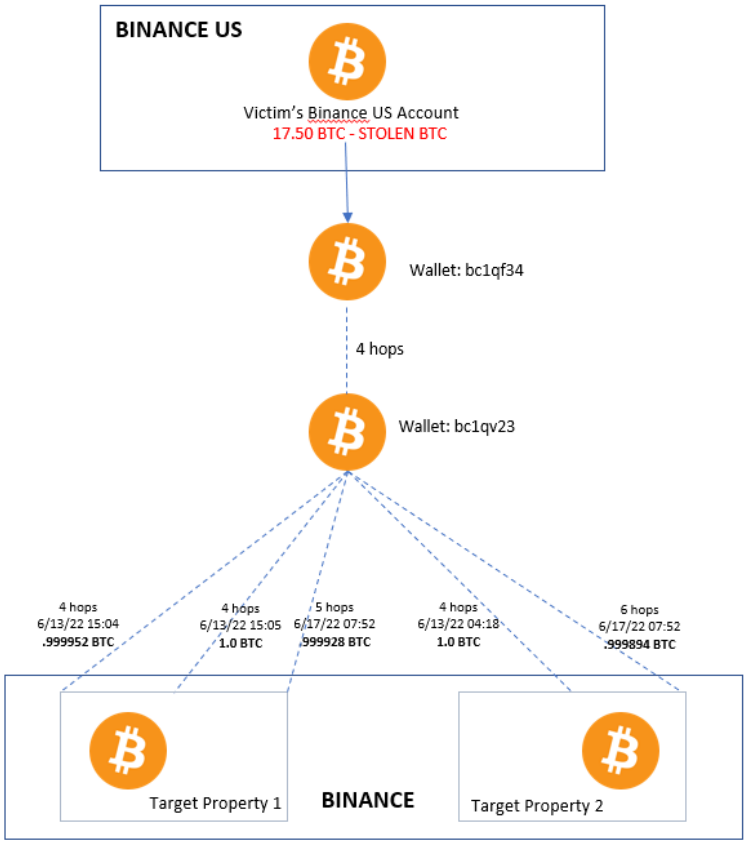
b. 5/16/2022 – Withdrawal 13.97166847 (bitcoin) to wallet "**bc1ql8a**"

c. 5/23/2022 – Withdrawal 2.53926749 (bitcoin) to wallet "**bc1qwed**"

25. Records from the Victims' bank accounts showed that between April 13, 2022, and May 20, 2022, $1,195,000 was transferred from the Victims' U.S.-based Wells Fargo bank account and credited to a Binance US customer account registered in Victim A's name (the Victims' Binance US Account). The following description of the movement of the stolen funds does not attempt to outline all funds flowing out of the Victims' Binance US Account, but rather those funds that were identified moving to Target Properties 1, 2, 4 & 5. The remaining funds from Victim's Binance US Account were traced to Target Property 3, unhosted wallets, other virtual currency exchanges, or to wallets operated by service providers or merchants.

Analysis of Victim Money Transferred to Target Property 1 and Target Property 2 via Victims' Binance US Account

26. Open source bitcoin blockchain analysis revealed that the money belonging to the Victims was transferred out of that account (the Victims' Binance US Account) in three separate transactions. The movement of funds from the first transaction is depicted in the following graph:



27. As detailed below, approximately $107,073, valued as of the date the virtual currency reached the destination wallets, was transferred through a series of intermediary wallets to two virtual currency addresses starting with **19amBvv** and **126FHS7**, which are truncated versions of the addresses associated with Target Property 1 and Target Property 2, respectively.

a. On April 22, 2022, 17.497852 bitcoin was transferred from Victims' Binance US Account and to a wallet address starting with **bc1qf34,** which was described above in Paragraph 24, subsection a.

b. According to blockchain analysis, between May 2 and May 10, 2022, the stolen funds were transferred through a series of 4 hops (*i.e.*, separate

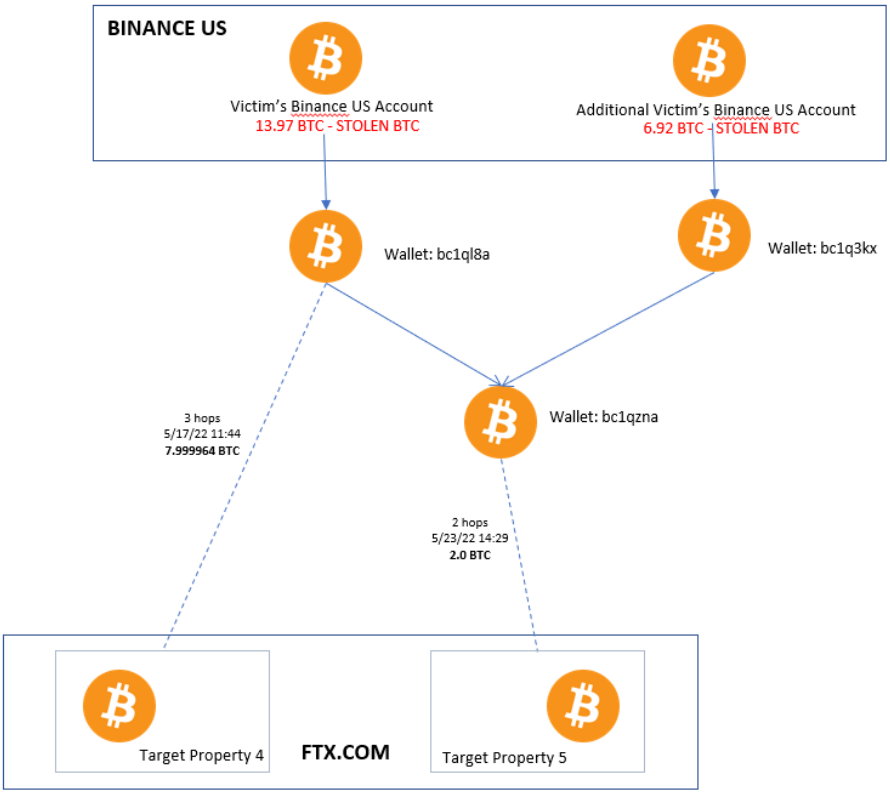
transactions) until on May 10, 2022, 5.0 bitcoin was transferred to address starting with **bc1qv23**.

c. According to blockchain analysis, at this point the stolen funds were split, through a series of transactions, into five separate deposits on June 13, 2022 and June 17, 2022, into either address **19amBvv** associated with Target Property 1, or address **126FHS7** associated with Target Property 2.

d. The transfers of stolen funds into Target Property 1 equaled 2.99988 BTC, which was equivalent to $64,607 at the times of the transactions. The transfers of stolen funds into Target Property 2 equaled 1.999894 BTC, which was equivalent to $42,466 at the times of the transactions.

Analysis of Victim Money Transferred to Target Property 4 and Target Property 5 via Victims' Binance US Account

28. The movement of funds from the Victims' Binance US Account to Target Properties 4 & 5 is depicted in the following graph:



29. As detailed below, approximately $294,512, valued as of the date the virtual currency reached the destination wallet, was transferred through a series of intermediary wallets to two virtual currency addresses starting with **3DHSTHF** and **3QdA3vx**, which are addresses associated with Target Property 4 and Target Property 5.

a. On May 16, 2022, 13.97166847 bitcoin was transferred from Victims' Binance US Account and deposited into a wallet at an address starting with **bc1ql8a**.

b. According to blockchain analysis, on May 16 and May 17, 2022, 8 BTC was transferred from **bc1ql8a**, through a series of three transactions, and was ultimately transferred (minus transaction fees) to address **3DHSTHF**, which is associated with Target Property 4.

d. According to blockchain analysis, also on May 16, 2022, 5.97164237 bitcoin from **bc1ql8a** was transferred to an address starting with **bc1qzna**. Only one other transaction deposited funds into **bc1qzna**, with 5.918391 BTC being sent on May 17, 2022, from an address starting with **bc1q3kx**. The **bc1q3kx** address received all of its funds from a transaction out of a Binance US Account on May 12, 2022. Records from Binance US revealed the owner of the account that sent funds to **bc1q3kx** was another US citizen residing in a different district. FBI conducted an interview of this additional account holder (hereinafter referred to a Victim C) determined that they had been victimized in a very similar fraud scheme. Like the Victims, Victim C contacted who they believed to be Microsoft and were told that their money was at risk due to hackers accessing their accounts. Like the Victims, Victim C was instructed to set up a Binance US account (hereinafter "Victim C's Binance US Account") and was instructed by the scammers to wire funds from Victim C's business account. From there, the scammers initiated a number of withdrawals to destination wallets completely liquidating Victim C's Binance US Account. In total, Victim C was defrauded out of $200,000.

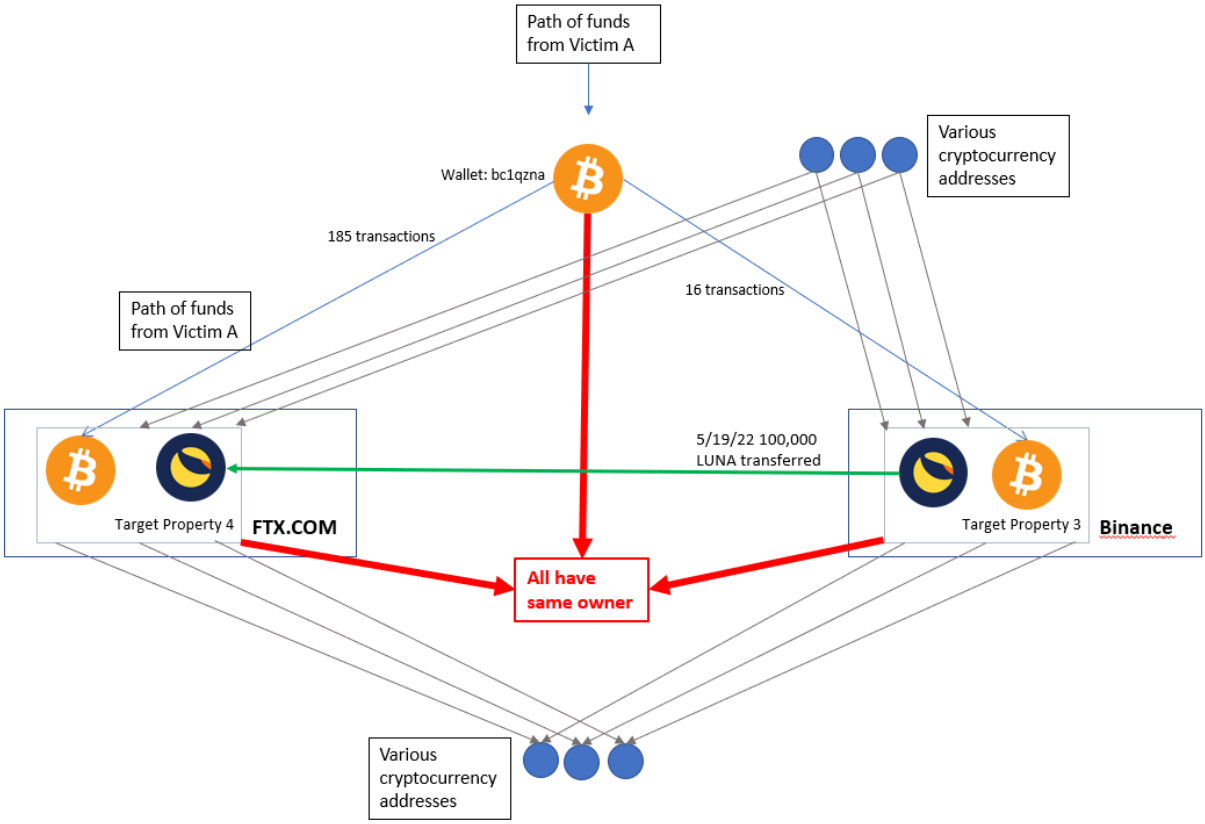
e. According to blockchain analysis, on May 23, 2022, the commingled funds in **bc1qzna** were sent via two transactions to an address starting with **3QdA3vx,** which is associated with Target Property 5. While the separation of funds from the Victims' Binance US Account and Victim C's Binance US Account was not discernable at this point, the funds that were traced forward made

it clear that the funds were collated and part of the same scheme and money laundering pipeline.

f. The transfers of those stolen funds into Target Property 4 equaled 7.999964 BTC, which was equivalent to $236,561 at the time of the transaction. The transfer of stolen funds into Target Property 5 equaled 2.0 BTC, which was equivalent to $57,951 at the time of the transaction.

Fraud Scheme Funds and Target Property 4 Links to Target Property 3

30. Over the course of the investigation, law enforcement identified an additional account at Binance that was tied to this fraud scheme, as well as directly tied to the Target Property 4 by ownership. Transactions involving bitcoin addresses already identified in the laundering scheme frequently involved a virtual currency address starting with **1HBXm9v**, which is associated with Target Property 3. The graph below depicts the transactions that link parts of the identified money laundering scheme with Target Property 3:



31. Several patterns of transaction behavior linked Target Property 3 with Target Property 4. FTX.com provided communications the exchange had with the owner of Target Property 4 in the form of customer support tickets. The owner of the account contacted FTX.com in May of 2022, questioning why the account was frozen. FTX.com staff replied that it was due to incoming transactions from addresses flagged for abuse complaints. FTX.com staff asked the account owner to verify multiple transactions from wallet address **bc1qnza**. The account owner claimed that those transactions were legitimate because they owned the **bc1qnza** wallet personally. FTX.com then continued to ask about transactions into the **bc1qnza** that were flagged for abuse complaints.

32. Of note, the **bc1qnza** address received funds from the Victims' Binance US Account and passed them to Target Property 4. In total, 185 separate transactions were

identified as flowing from **bc1qnza** to Target Property 4. Simultaneous to the 185 transactions to Target Property 4, an additional 16 transactions were identified that originated from **bc1qnza** to Target Property 3 was well.

33. An analysis of records provided by Binance and FTX.com related to Target Property 3 and Target Property 4 identified multiple commonalities. Foremost among those common points was the fact that the accounts were opened using the same name and same personal identification documentation.

34. Additionally, common counterparties were identified in the transaction histories from Target Property 3 and Target Property 4. Multiple sending addresses across various cryptocurrencies sent funds to both Target Property 3 and Target Property 4 within the same time span. Likewise, Target Property 3 and Target Property 4 sent funds in various cryptocurrencies to the same receiving addresses within the same time spans. In my training and experience, this parallel transaction history indicates the accounts were utilized for similar purposes and were likely controlled by the same individual(s).

35. Finally, there was evidence that funds were directly exchanged between Target Property 3 and Target Property 4. As an example, on May 19, 2022, Target Property 3 sent 100,000 LUNA, which was the cryptocurrency associated with the Terra blockchain, to Target Property 4.

36. During the course of the investigation, I learned that the Charlotte FBI Field Office was investigating a virtual currency wallet associated with Target Property 3. In summary, on or about March 21, 2022, the Victim from the Charlotte FBI case

(hereinafter "Victim D"), who was a victim in a similar fraud scheme, was instructed by an unknown subject to open an FTX.us online banking personal account and to send a wire of $50,000. The amount of money was determined because $50,000 was the minimum amount of money that could be sent on an FTX personal account. Victim D made several wire transfers from Victim D's State Employees Credit Union account to the FTX account. Whenever Victim D went to the bank to wire money, "Alan" or another person called "Kevin," would remotely print a form on Victim D's printer to give to the teller. They instructed Victim D to rotate branches and not to go to the same branch. Victim D went to three different State Employees Credit Union branches during this period and continued to send wires because Victim D was being informed by the scammers that the wires were being denied. They would print out false account balances to calm Victim D down and to mislead Victim D into thinking Victim D's account balances had not changed. In total, Victim D was defrauded out of $352,520.

37. FBI Charlotte obtained records from FTX and determined the funds were converted from U.S Currency to Tether ("USDT"), a stablecoin backed by U.S. dollars. They were able to trace the funds to a wallet associated with Target Property 3. In addition, the same individual is the account holder of Target Property 4 and of BTC address **bc1qnza**. Based on my training and experience and the information provided by other law enforcement officers related to the fund tracing, it is my belief that Target Property 3 and Target Property 4 are being used for the purpose of laundering funds in fraud scheme outlined throughout.

Conclusion

38. Based on the facts alleged above, there is probable cause to believe that the Defendant *in rem*, namely all property seized from Target Properties 1, 2, 3, 4 and 5, is subject to civil forfeiture as proceeds of wire fraud committed by the scammers against Victims A, B, C, and/or D, and/or property traceable to such proceeds, and also subject to civil forfeiture as accounts and property involved in money laundering and/or traceable to property involved in money laundering, given the comingling of the wire fraud proceeds with other property in the above-described accounts. *See* 18 U.S.C. §§ 981(a)(1)(A) & (C).

Execution of Seizure Warrants 1:22-mj-00081-MMS and 1:22-mj-00082-MMS

39. On October 6, 2022, Anchorage FBI seized the assets from the TARGET PROPERTIES, including the Defendant *in rem*, pursuant to seizure warrants 1:22-mj-00081-MMS and 1:22-mj-00082-MMS.

Request for Warrant for Arrest In Rem

40. Upon the filing of this complaint, the plaintiff requests that the Court issue an arrest warrant in rem pursuant to Supplemental Rule G(3)(b), which the plaintiff will execute upon the defendant property pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(c). Because the Defendant *in rem* is not real property and is in the government's possession, the clerk must issue the warrant. Supplemental Rule G(3)(b)(i).

Claim for Relief

41. Plaintiff repeats and incorporates by reference the paragraphs above.

42. By the foregoing and other acts, there is probable cause to believe that the Defendant *in rem* is subject to forfeiture to the United States of America under 18 U.S.C. §§ 981(a)(1)(A) & (C).

WHEREFORE, the United States of America prays that:

a. A warrant of arrest for the Defendant *in rem*, be issued;

b. That due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed;

c. That judgment declare the Defendant *in rem* to be condemned and forfeited to the United States of America for disposition according to law;

d. And that the United States of America be granted such other and further relief as this Court may deem just and equitable, together with the costs and disbursements of this action.

RESPECTFULLY SUBMITTED this 13th day of April, 2023, in Anchorage, Alaska.

S. LANE TUCKER
United States Attorney

s/ Seth M. Beausang
SETH M. BEAUSANG
Assistant U.S. Attorney
United States of America

CERTIFICATE OF SERVICE

I hereby certify that on April 13, 2023, a true and correct copy of the foregoing was served on the following:

Barbara Mazza
Terry and Ronald Hansen
Theresa M. Riocci
Guarav Dhingra
Gaurav Pahwa
Kunal Almadi
Kiran Arora

s/ Seth M. Beausang
Office of the U.S. Attorney

VERIFICATION

I, Frank D. Reid, Jr., hereby verify and declare under the penalty of perjury that I am a Special Agent of the Federal Bureau of Investigation, that I have read the foregoing Verified Complaint for Forfeiture In Rem and know the contents thereof, and that the matters contained in the Verified Complaint are true to the best of my knowledge and belief, and are based upon my personal knowledge; interviews of witnesses; review of documents and other evidence; conversations with other law enforcement personnel to include forensic accountants knowledgeable about cryptocurrency; and training, experience and information received concerning the use of computers in criminal activity. This complaint does not include all the facts that the FBI learned during the course of its investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Executed this 7 day of April 2023, in Juneau, Alaska.

Frank D Reid, Jr.
FBI Special Agent

Declarations have the same legal force as affidavits. 28 U.S.C. § 1746